PUBLICATION DATE: 14. 10. 92
(further bibliographic data on next page

Identification of Individuals by Means of Facial Thermography

Francine J. Prokoski
Robert B. Riedel
Jeffrey S. Coffin

MIKOS, Ltd.
Center for Innovative Technology, Tower Suite 300
2214 Rock Hill Road
Herndon, VA 22070

ABSTRACT

MIKOS Corporation has patented the use of thermal imaging systems for recognition of individuals through analysis of "elemental shapes" in facial thermograms. MIKOS has demonstrated that facial thermograms are unique to the individual, and has developed methods and systems for positive identification aimed at access control, intruder detection, surveillance imagery analysis, secure teleconferencing, access to secure computer systems, and related markets. MIKOS' FACES™ system [Facial Access Control by Elemental Shapes] utilizes the infrared emissions produced from individual's faces to uniquely identify the individual.. The data may be collected passively and instantaneously, from a distance, and with no risk to the individual. It is therefore particularly well-suited for security applications. The thermal pattern on the face surface at any instant is influenced by and indicative of: the gross anatomy of the individual's head, the ambient environment, the vascular system of the person, any appliances (such as facial hair, makeup, glasses, or bandages), and any immediate contact with other objects (such as an ice pack, handkerchief, or cigarette). By proprietary analysis of the produced image, characteristic features can be extracted from the thermal image and used to uniquely identify an individual, even in complete darkness, and in spite of all the variables mentioned. The accuracy and robustness of the resulting identification system provides for its use in general security systems, where it provides a non-contact, hands-free and on-the-fly positive identification capability especially suited to high throughput and emergency conditions such as rapid evacuation procedures. The FACES™ system also provides the only available technique for continuous verification of presence and identity of persons accessing secure broadcasts, logged-on to secure computer systems, or participating in secure teleconferences. The system requires no additional cooperation from the user, except for watching the screen. The FACES™ system will cause the screen to blank, or the network to be logged-off, if the authorized person stops watching the screen or if an unauthorized person joins the audience. Particular versions of FACES™ systems include the FaceCard™ and ASAP™ systems. FaceCard™ is a card-based system, which utilizes a photo-ID badge on which is also encoded information from the individual's facial thermogram. FaceCard™ control can be installed for any entry way without the need for connection to a central database. The system merely compares the encoded thermogram information with that of the presented face. Since it is not possible for one person to mimic another's facial thermogram, lost cards do not present a security risk. The card does double duty as a standard ID badge. The ASAP™ [Airport Secure Area Protection] System offers dual mode surveillance/access control. Airport personnel wear or carry FaceCard™ photo ID badges, which are used to obtain access to secure areas. At any time the infrared camera is not actively processing an access control request, it is surveilling the area. Programmable options include: change detection and intruder detection. Current expansions of the techniques will facilitate matching between infrared imagery, such as collected from surveillance tapes, with mug shots and other standard video imagery.

Background

The problem of proving the identity of an individual or verifying whether an individual is the person he claims to be, is a common one faced continually by individuals, businesses and governments. Methods for positive identification of an individual usually include reliance upon: possession of a restricted article (such as a passkey), knowledge of restricted information (such as a password), or physical appearance (such as matching a reference photo).

Security based upon possession or knowledge may be compromised without discovery, since the information or article may be extorted from its rightful owner. The third category, commonly referred to as biometric techniques, is considered less vulnerable to mistaken identity, and is the only type which provides positive identification of the individual; the other two types providing only identification of the restricted article or information. The best known biometric technique, and the one considered most secure, is fingerprints.

Many security systems and methods have been developed which involve finger prints and/or palm prints, which are believed to be unique to an individual. NEC, Morpho, De La Rue, Identix and Printrak all offer fingerprint reading systems. The first three listed sell AFIS systems [Automated Fingerprint Identification Systems] used by federal, state and municipal police forces to process millions of prints per day. Fingerprints remain the only positive form of identification routinely allowed as evidence in court. However, their use for real-time access control is limited by the accuracy of non-ink imaging techniques, by the maintenance requirements associated with the need for clean contact surfaces and by the cost, time and inconvenience required. Identix has successfully developed a low cost, quick comparator for single fingerprints, and has implemented the system for access control use. Its accuracy, however, is below what is obtained through analysis of a full set of ten inked prints. Palm prints can be considered a less accurate version of fingerprints, having the same limitations. Both may be forged through various means, including the use of latex or tapes to transfer prints from other surfaces or from the hands and fingers of other persons. Therefore, although fingerprints offer very high accuracy for identification, the use of single print readers in unattended locations is not advised when strict security is desired.

Other biometric techniques include retinal scans, pioneered by Eyedentify Inc., and measurements of body weight. The retinal scan procedure, although considered highly accurate, suffers from the reluctance of many individuals to put their eye on a common piece of hardware where it is exposed to laser light. The time and inconvenience required for the procedure is also considered a deterrent to its use in certain situations. Measurements of body weight have proven effective only in conjunction with other more precise identification techniques. In particular, use of a weight sensor can help assure that only one person at a time passes through an unattended access portal; a technique known as "anti-piggybacking". Table 1 summarizes the relative features of various biometric techniques. Only the FACES™ system offers: unique identification under any lighting or noise conditions, with non-contact, rapid processing of large numbers of people, and relative immunity from forgery or disguise.

Individuals identify one another primarily by recognizing their faces. It is therefore understandable that systems would be developed which would attempt to replicate how persons recognize one another. Although no commercial products yet exist which automatically recognize faces from photos or video images, various patents have been issued which utilize known photographic or other visual images for comparison with unknown images in order to automate the recognition task.

The "facial curve" method computes the curves (two or three dimensional) of an individual face taken from full-face, forty-five degree angle, and profile (ninety degree angle) which are then

3119-5/92

Proceedings

THE INSTITUTE OF ELECTRICAL
AND ELECTRONICS ENGINEERS

1992 International Carnahan Conference on Security Technology: Crime Countermeasures

October 14 -16, 1992

Atlanta Penta Hotel, Atlanta GA

EDITOR
LARRY D. SANSON

Sponsored by:

- IEEE Lexington Section, U.S.A.
- IEEE Aerospace and Electronic Systems Society, U.S.A.
- Georgia Tech Research Institute

In Cooperation With:

- Swiss Federal Institute of Technology, SWITZERLAND

IEEE

GTRI

stored on an identity card or in a data processing machine. Identification of the individual is performed by first visually comparing the photographs on the identity card to the individual presenting the card and then if desired, taking an image of the individual and automatically comparing by computer the curves stored on the identity card with curves derived from the image. In order to properly compare such an image with the computer data, however, the individual must be positioned and aligned in front of a glass screen.

The "facial measurements" method utilizes the ratios obtained from a set of measurements taken off of a facial image collected under relatively uncontrolled conditions, and finds the best match among small groups of known individuals constituting a target audience. The accuracy depends on the extent to which lighting and shadows are controlled and the geometry of the person's position relative to the camera or cameras.

Table 1
Comparison of Biometric Identification Techniques

	UNIQUE	NON-CONTACT	ON-THE-FLY	NON-COUNTERFEITABLE	ANY CONDITIONS
FACES™	✓	✓	✓	✓	✓
Face Photos		✓	✓		
Retinagrams	✓			✓	✓
Fingerprints	✓				
Voice Recognition	✓	✓			

Use of photographic imagery for identification is commonly known to have many limitations and vulnerabilities. Most important among them are the effects of lighting and shadow on the recognizability of an individual from picture to picture. Also, aging effects and the use of worn or surgical disguises such as the addition/removal of facial hair, dying or bleaching of hair, application of makeup, wearing of plumpers, false teeth and other oral appliances, and cosmetic surgery may render an individual unrecognizable when compared to a previous photograph. Worn and surgical disguises may also be used in a directed attempt to make someone look like someone else. Photographic techniques may not be able to detect the difference between an individual and an imposter, and often cannot distinguish between identical twins.

Several universities and companies worldwide are currently developing facial recognition systems based upon using the artificial intelligence technique of neural nets. These systems are "trained" to recognize certain faces by being given many images of each person taken under varying conditions, produced using photos, video images, artist's drawings, etc., to force the system to link all such images with the same individual. Depending on the processor speed and database storage size, current neural net recognition systems are being trained to recognize a population of individuals in groups of 200 or more.

Neural networks have a fundamental limitation in that each time a new object is introduced into the database to be recognized, the network must be re-trained. Therefore, it is usually necessary to partition large databases into smaller groups; otherwise, re-training could be a continual task, and the system could not operate. When used for applications such as access control, the training requirement may be prohibitively expensive and time consuming. In situations where many individuals must be enrolled in the system, and there is a high turnover of individuals being added to or deleted from the system, the downtime associated with re-training the system can be significant. Although certain of the developers are quoting high rates of accurate identification for their neural nets, given that the systems utilize only video images they remain vulnerable to disguise and to lighting conditions. Table 2 summarizes a comparison of video and infrared identification techniques.

Table 2
Comparison of the Vulnerabilities of Video and IR Systems

Effects	Video	IR
Illumination	Affects Accuracy	No Effect
Disguises	Vulnerable	Not Vulnerable
BTL Tampering	Vulnerable	Not Vulnerable
Cosmetic	Affects Accuracy	No Effect
Seasonal	Affects Accuracy	No Effect
Ageing/Surgical	Affects Accuracy	Less Affected
Price (1992)	under $5,000 / gate	over $5,000

Training of a neural network uses "fuzzy" logic, which means that variations are permitted in each parameter measured. The result is that neural net systems can recognize images which are not exactly identical to ones in the database; which differ, for example, in the distance and angle of the camera, growth or reduction of facial hair, wearing of glasses, hairstyle, etc. However, neural nets basically cannot recognize faces any better than humans can; they are fooled or defeated by poor lighting, disguises and major changes in appearance.

Certain sensors in routine use for medical imaging could possibly be used for identification. For example, dental x-rays have long been used for that purpose. In general, the potential for disguise or forgery is avoided by the fact that such sensors are imaging details which are below the skin's surface. Automatic interpretation of images from such sensors as: x-rays, CAT scans, nuclear magnetic resonance and other such invasive techniques can utilize the analysis methods invented by MIKOS. However, for general repetitive identification use, only passive, non-invasive techniques deserve consideration. The most amenable of those, and the biosensor which is used in the FACES™ system, is thermal imaging.

Because the thermograph operates at a distance from the subject and detects and records only radiant heat spontaneously emitted from the body surface, it constitutes a painless, non-invasive, passive method of recording body surface temperatures. Thermal measurements of individuals under repeated conditions are highly repeatable. The mean and standard deviation temperatures of a group of individuals over a period of several months were 30.8° +/- .032°C with a coefficient of variation of 0.1%. In healthy individuals, there is general symmetry of the face, with the degree of asymmetry being only 0.18 +/- 0.18°C for foreheads and 0.18 +/- 0.18°C for cheeks.[1] Such repeatability of absolute thermal measurements insures the repeatability of the elemental shapes required for the MIKOS analysis. Thermal images collected by the inventors over a 20 year period demonstrate the persistence of the elemental shapes, in the individuals studied, for at least that duration.

MIKOS is the only company performing facial identification through analysis of thermal images. This capability is inherently more accurate and more robust over varying lighting and environment conditions than is the use of video images. Since the use of a thermal imaging camera is still significantly more expensive than the use of a video camera, comparable costing is the major limit to the Company's ability to capture market share in the facial identification market. A secondary limitation is the desire in certain instances to record a visually recognizable image of the individuals

identified. In those instances, a dual-band camera can be used which records both visual and infrared images; this, of course, further increases the price differential between thermal/video and pure video identification systems.

DOD Sponsorship of IR Systems Development

The thermal imagers used in the FACES™ system were initially developed for "Smart Bomb" use in targeting weapons deployments. Such devices use detector arrays operating at cryogenic temperatures, typically producing an image whose spatial resolution is equal to that of a standard TV picture, and providing temperature discrimination sensitivity of about 0.1° F. The military grade imaging systems, including the cryogenic coolers, typically cost $100,000 or more.

Recent declassification of portions of the federal government's uncooled infrared sensor program has facilitated consideration of that technology. MIKOS has subsequently evaluated pre-production prototype room temperature IR cameras for FACES™ applications. With modification to its analysis procedures, MIKOS was able to demonstrate effective use of the uncooled camera for access control applications. As a result, MIKOS can now anticipate offering FACES™-systems at a price below $7500 starting in 1994, with further reduction to $2500 in 1997 and $1500 in 1999. By 2000, a positive facial ID system could sell for less than $1000 per access point. Other developing technologies for direct translation of IR into video signals may also be viable, and at even lower costs. At these price levels, a broad range of government and commercial applications, including point of sale and ATM terminals, will be marketable.

Market for Biometric Systems

MIKOS' primary business sector is the design, manufacture, distribution and servicing of identification and access control systems. The market for such devices and services includes all facilities which seek to restrict access to physical areas, distribution systems or information files. Installation locations include: weapons storage areas, ATM cash-dispensing machines, and government classified data bases, respectively. The customers responsible for access control at those locations include: federal, state and local government agencies; banks and other commercial and retail establishments; and R&D laboratories seeking to restrict dissemination of information. Table 3 lists some of the most immediate potential applications for positive identification systems.

TABLE 3
Applications for Positive Identification Systems

ACCESS to RESTRICTED AREAS:

Airport Cargo, Ticket and Baggage Areas
Airport Control Towers, Refueling and Maintenance Areas
Marine Port Facilities
Bank Vaults, Safety Deposit Boxes, Cash Windows and Wire Transfer Areas
Embassies and Corporate Offices in Foreign Countries
Nuclear Facilities, Conventional Power Stations and Grid Control Stations
Munitions and Hazardous Materials Storage Areas
Museums and Warehouses storing Valuable Items
Government File Archives and Computer Centers
Corporate Archives and Computer Centers
Postal Distribution Centers, Government and Private Carriers
Clean Rooms in Hospitals and in Medical and Genetic Engineering Labs
Blood Banks, Tissue Banks and Forensic Labs
Research and Development Facilities

ACCESS to DISTRIBUTION of GOODS and SERVICES

Automatic Teller Machines - Cash
Point of Sales Terminals - Goods and Credit
Welfare Agencies - Food Stamps, Cash
Drug and other Clinics - Medication
Prisons - Justice based upon Past Record
Computer Networks - Electronic Funds Transfer
Hospitals - Treatment

ACCESS to RESTRICTED INFORMATION

Company Proprietary Data, Plans and Forecasts
Government Reports and Regulations in Progress
Classified Government Files
Financial Securities Transactions
R&D Technical and Business Data
Medical and Personnel Records
Law Suit Preparation Files
Patent Applications
Wills and Personal Papers
Competitive Proposals
Trial Evidence

The market volume is driven by both actual and perceived increases in violent crime, drug abuse, criminal population, disenfranchised immigrants and terrorist groups. Repeat offenders in US prisons account for more than 85% of felonies committed in this country. Lack of resources to build additional prison space causes many of them to be released to society without rehabilitation. More than 40% of convicted felons have drug dependencies, which in most cases survive the period of incarceration.[2] The need to finance their drug habits keeps most such individuals caught within a spiral of escalating criminal activity.

Given an increasingly transient population, with resulting turnover of employees, the task of controlling personnel access to secure areas of facilities, or to restricted information or systems, becomes increasingly important but also increasingly difficult — particularly at large facilities. The use of guards for access control becomes less secure when the guards themselves are transient or may have a history of drug use. The use of ID badges, passkeys or other techniques in addition to guards is becoming more common. However, the combined costs of having both technical and guard access controls at the same points is not only excessive in most cases; it may offer no greater security than either system alone.

The MIKOS technology, as incorporated into the FACES™ systems, has the following significant attributes and advantages over competing techniques:

1. It provides identification over short or long distances, in cooperative or covert deployments.
2. It provides a method for uniquely identifying individuals under all lighting conditions, including total darkness.
3. It requires little or no cooperation by the user.
4. It is totally passive, non-contact and non-invasive. In particular, it involves no need to place any part of the body in contact with any part of the system. It therefore offers no actual or perceived risk of infection or injury to the user.
5. It thereby offers reduced risk of vandalism, and requires no special maintenance of parts which come in contact with the users.
6. Due to its relative immunity from forgery deception, it provides convenient, unattended, highly secure identification of individuals seeking to use automatic teller machines, or transact business at automatic point of sales terminals.
7. The very high degree of security provided, coupled with the fact that the database of thermal images provides no definitive information on race, sex, or age, makes the system ideal for access control to vaults, safe deposit boxes, private locations, and classified data. The database of authorized persons does not provide identity information which could be used to extort cooperation by such authorized persons.
8. The FACES™ technology provides a hand-free positive identification capability for access to clean room areas, such as genetic engineering labs, [illegible]

to be avoided, or where no items such as keys or badges may be brought from outside.

9. The systems are cost compatible with other high security biometric identification systems, such as those comparing a full set of fingerprints. In addition, the FACES™ systems can often serve additional functions, such as surveillance, which make them cost effective even to access control users not requiring absolute security.

10. Investigation is currently underway to evaluate the use of uncooled infrared sensor technologies for the FACES™ System. Initial evaluations indicate that the uncooled technology can be adapted effectively for certain short-range applications. This will lead to a $5000 FACES™ system within the next three years, and a $2500 system within five years. By the year 2000, the FACES™ system will be less than $1000. At each stage in the price reduction, additional markets will open.

Nature of the Identification Technology

The Company's proprietary technology involves the use of biosensor data for uniquely and automatically identifying individuals. Due to the connectedness of the physiological systems of the human body, "elemental shapes" can in general be derived from any biological sensor data which can be represented as an image. The elemental shapes and their locations provide an identification capability. Biosensors which produce very detailed localized data, such as high resolution infrared imagers, can result in unique identification of an individual from the determination of elemental shapes and their distribution.

"Elemental shapes" have been discovered and defined by the MIKOS inventors as contours in space, whose shapes are determined by the extent, intensity, and duration of output from a biosensor as represented by an image. An elemental shape may be used as a fractal to perform compression of the data from the biosensor. By selecting elemental shapes located at areas of greatest concern, image compression may be performed with negligible risk that the most essential information will be lost through compression and decompression. Furthermore, these elemental shapes may be ranked or classed much in the same manner as fingerprint features. Hierarchical search criteria based on the elemental shapes may then be used to search a database of compressed images to locate a match between known and unknown subjects; to identify changes from time to time in a known subject; or to search for a known condition through a large database of subjects.

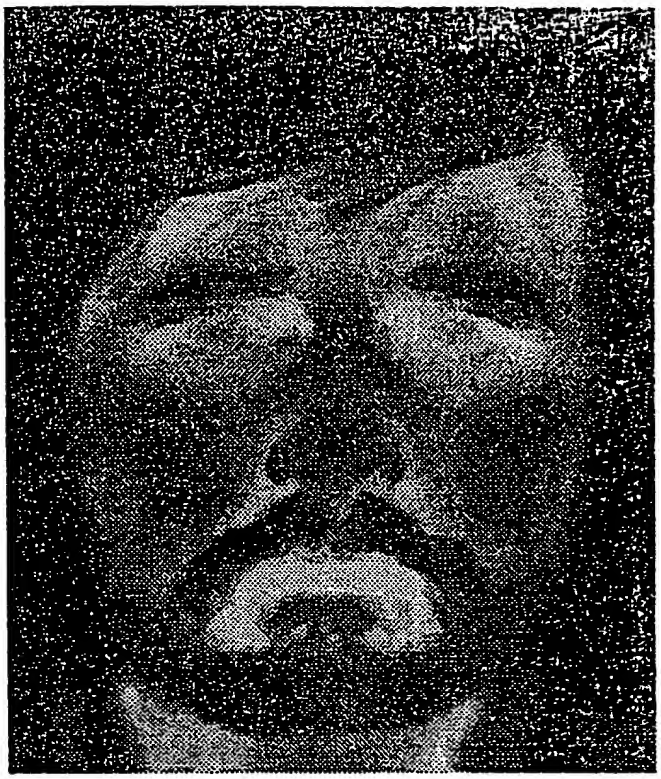

Figure 1. Facial Thermogram

Figure 1 is a facial thermogram which shows the image produced when 65,000 individual temperature measurements are recorded across the face. By proprietary analysis of the produced image characteristic features can be extracted from the thermal image and used to uniquely identify an individual, even in complete darkness. The accuracy and robustness of the resulting identification system provides for its use in general security systems, where it provides a non-contact, hands-free and on-the-fly positive identification

Figure 2. Processed Facial Thermograms

Figure 2. Processed Facial Thermograms (continued)

capability especially suited to high throughput and emergency conditions such as loss of power, total darkness and rapid evacuation procedures.

Figure 2 presents four processed facial thermograms, which represent the amount of difference normally found among individuals. Due to its primary application as an unattended secure access control device, the FACES™ system automatically normalizes for various operational parameters which affect apparent face size, orientation and distributions of apparent temperatures. Due to its potential use for identification of individuals over long period of time, the system is designed to not be confused by the growth or reduction in facial hair, or by sun tan, fever or exposure to cold. Unlike the use of thermography for medical analysis, the present invention does not require a clinical setting in which the individual is acclimated to a constant ambient temperature.

A facial thermogram is the resultant three-dimensional image obtained by scanning each minute section of the face onto one or more detectors which are sensitive in the infrared range. The most commonly used medical thermal imagers produce an image which comprises approximately 60,000 individual heat recordings. The magnitude of that number, plus the size of the facial area being imaged, are more than ten times larger than the number of details (minutiae) and area associated with fingerprint analysis. Therefore, although no direct large-scale comparison has been made, the FACES™ system is believed to generate unique images for each person, and to provide very high identification accuracy, equalling or surpassing that of fingerprints, even when only a partial face is imaged.

Figure 3 presents the facial thermograms of identical 14 year old twin girls. The contours and fractal dimensionality of the elemental

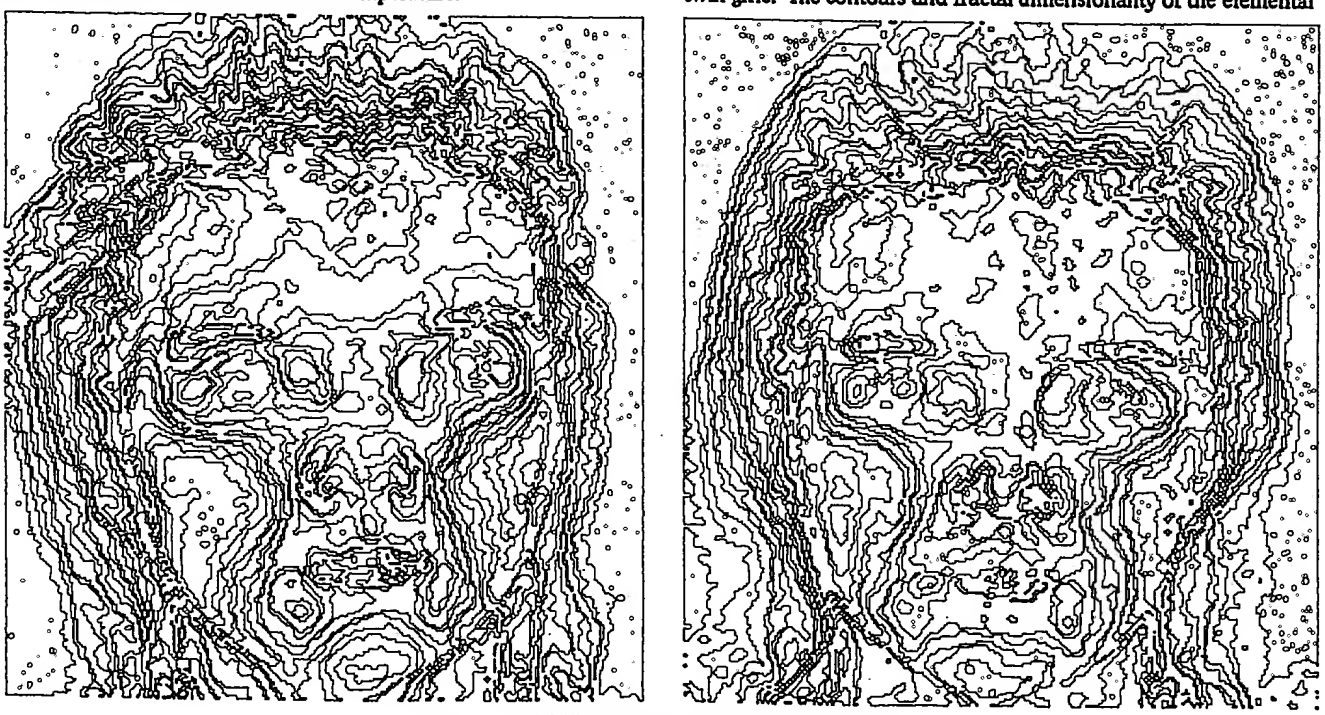

Figure 3. Facial Thermograms of Two Identical Twins

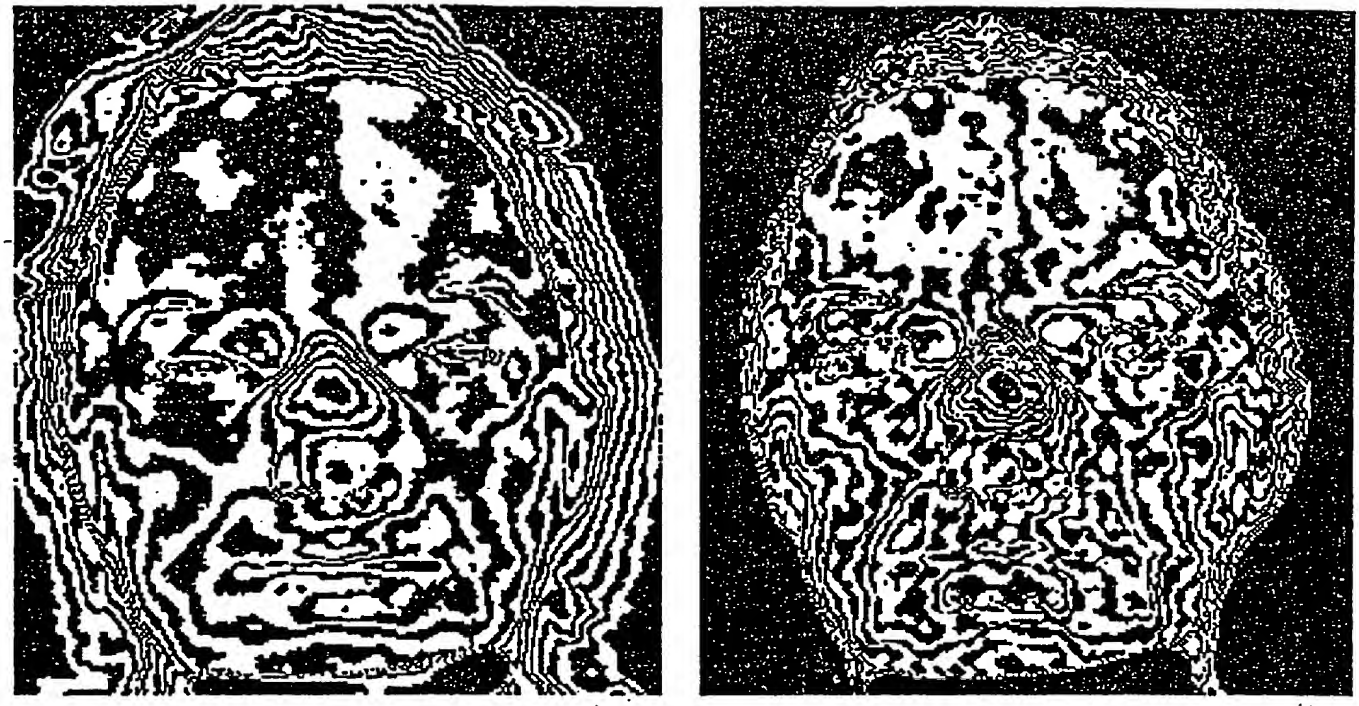

Figure 4. Facial Thermogram before (left, above) and after Alcoholic Drink

shapes in the sinus areas are particularly distinct. The elemental shapes in the cheek areas are also different. Given those four areas were used for identification, as in the usual embodiment of the MIKOS technology, the system readily distinguishes between the twins.

The use of drugs and alcohol produces marked changes in facial thermograms, as evidenced by the before and after images of Figure 4, which pertain to the ingestion of 8 oz. of Harvey's Bristol Creme by a non-alcoholic. Research is on-going by MIKOS Ltd. to characterize the thermograms of three major population divisions: current or former addicts; non-addicts; and abstainers. Along with additional studies of the effects of drugs and alcohol on particular individuals, the results will be used to develop facial thermography as a pre-screening technique for drug and alcohol use by persons enrolled in databases and for whom baseline data exists [such as airline pilots and persons in rehab programs as a condition of parole]. Future use of facial thermograms during booking of criminal suspects, and related indicators of suspected drug usage at the time of arrest, may follow that research.

References

[1] Sumio Uematsu et al., "Quantification of Thermal Asymmetry", Journal of Neurosurgery, Vol. 60, No. 4, October 1988.

[2] US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, Correctional Populations in the United States, 1989, 1991. NCJ-130445.

[3] Margaret Abernathy and Sumio Uematsu, "Thermography in Cerebralvascular Disorders and Headache", Medical Thermology, Part Two, American Academy of Thermology, Georgetown University Medical Center, Washington D.C., 1986.

[4] Howard Souchurek, "Medicine's New Vision", National Geographic, Vol. 171, No 1, January 1987, pp. 2 - 40.

[5] Peter Tal, Method and Apparatus for Uniquely Identifying Individuals by Particular Physical Characteristics and Security System Utilizing the Same, U.S. Patent No. 4,975,969, 4 December 1990.

[6] F.D. Shepherd, W.S. Ewing, B.R. Capone and R.W. Taylor, "Platinum Silicon Staring Sensor Evaluation", Proceedings of SPIE, Thermal Imaging, Vol 636, 1986.